Ransomware on the rise: Protect your WFH, telehealth gaps and update your IT plan

by: Roy Edroso

Effective Nov 19, 2020

Published Nov 23, 2020
Last Reviewed Nov 19, 2020

Ransomware, a bane of health care providers for years, has gotten even worse, leading to steeper consequences for providers who have been hit by it. Adding to the challenges, the pandemic-induced wave of work-from-home (WFH) orders has made attacks easier for crooks. It's time to double down on your defenses.

On Oct. 28, HHS and the FBI, together with the U.S. Cybersecurity and Infrastructure Security Agency (CISA), announced in a joint report that they had "credible information of an increased and imminent cybercrime threat to U.S. hospitals and health care providers."

Cybercriminals have "continued to develop new functionality and tools, increasing the ease, speed and profitability of victimization" and increasingly aim it at the "Healthcare and Public Health Sector (HPH) É often leading to ransomware attacks, data theft and the disruption of health care services," the report states.

Ransomware is a kind of malware that began to emerge in the health care world in 2015 (*PBN 5/4/15*). It is spread and launched by links in phishing emails opened by unwary employees and locks down connected computer systems; its operators demand payment, usually in cybercurrency such as bitcoin, to release the files.

By 2016, ransomware was so prevalent in health care that HHS' Office for Civil Rights (OCR) was obliged to rule on its HIPAA impact, announcing that unless the provider who was attacked could prove otherwise, ransomware attacks would be considered a reportable breach (*PBN 8/8/16*).

The latest offender

The impact has only increased in recent years, and in response HHS laid out "Voluntary Cybersecurity Practices" with which practices might defend against it in 2019 (*PBN blog 1/7/19*). The current report warns providers that a major cybercriminal enterprise called TrickBot "now provides its operators a full suite of tools to conduct a myriad of illegal cyber activities," among them the recent ransomware varieties Ryuk and Conti.

Virtual private network company NordVPN reports that Ryuk is "believed to be behind the recent ransomware attack on Universal Health Services (UHS), running approximately 400 hospitals and care centers across the United States and the United Kingdom, making it one of the largest medical cyberattacks in U.S. history."

And it's not just hospitals that have to worry.

"While hospitals, due to their sheer volume, are larger treasure troves of information, often independent physician practices could be tempting targets because most don't have large dedicated IT departments to focus on cybersecurity protections for the practice," cautions Rich Temple, vice president and CIO at Deborah Heart and Lung Center in Brown Mills, N.J.

Health care faces heightened risk

Ransomware is booming because it's a quick way to make money — sometimes lots of it.

"I have seen demands for ransoms rise tenfold in 2020," says Oli Thordarson, CEO and founder of Alvaka Networks in Irvine, Calif. "I saw my first $20M ransom last month."

Also, ransomware has been "commodified" — that is, it's sufficiently mature that successful hackers are selling kits on the Dark Web so others can use it, according to Sue C. Friedberg, co-chair of the Cybersecurity and Data Privacy Group at Buchanan, Ingersoll & Rooney in Pittsburgh. Ultimately, that means there are more criminal entrants in the market.

But also ransomware has gotten more intense, and hackers are able to extract data more aggressively than before, says Kristen Dauphinais, head of U.S. cyber and technology with Beazley in Dallas.

"When we really started seeing ransomware events in earnest, they were very simple, kind of smash-and-grab jobs," Dauphinais says. "You'd have somebody click on a link that would allow the malware into the system, and the files would be encrypted."

But now, “it’s become much more complicated and invasive,” Dauphinais says. “Ransomware is getting into the system, but the bad actors are sitting in that system and waiting much longer to act. Meanwhile they’re watching traffic to see how people communicate there and where information systems are and aren’t protected, in addition to getting the malware onto the backups.”

This allows the crooks to feel their way around the system, find data they might not have bothered to seek out before, and exfiltrate, or extract, it before finally announcing the lockdown of the victim’s entire system.

“We are now seeing situations where the ransomware may actually be a parting gift, if you will, after other access and activity in the system,” says Pamela E. Hepp, a shareholder and the other co-chair of the Cybersecurity and Data Privacy Group at Buchanan, Ingersoll & Rooney. “And they may have been there for a period of time, but had not been detected until the ransomware attack. In some respects, the ransomware attack may be intended to hide their tracks, and when you get in and do the analysis, you realize that it was a parting gift.”

The exfiltrated medical and personal data can be very valuable to thieves. For example, it enables medical identity theft, which “allows a fraudulent person to receive healthcare benefits they’re not entitled to, as well as access to prescription history,” says Steve Tcherchian, chief information security officer at cybersecurity analytics company XYPRO in Simi Valley, Calif. “This enables thieves to purchase prescription drugs on a patient’s behalf, which are then resold online on black market websites.”

Also, hackers may separately ransom sensitive personal data skimmed in the attack and threaten to “post the data or make it available either for sale or just to make it available, as an embarrassment to the entity,” Friedberg says.

Where the problems lie

Experts agree that the pandemic-inspired WFH and telehealth trends have left medical entities more vulnerable, as home workers on laptops and providers interfacing with patients on Skype improvise their own approaches to security, relatively unmediated by their company’s IT department.

“The shift to WFH was sudden and unplanned by most firms,” Thordarson says. “The IT teams, and even some contractors, were not adequately staffed with the right skills to do this properly and securely.”

Slackened security on telehealth since OCR allowed providers to use non-HIPAA-compliant software and devices has also amplified insecurities.

CISA issued a ransomware guide in September listing protocols it recommends for defense. Many are technical in nature — for example, to discourage phishing they suggest “disabling macro scripts for Microsoft Office files transmitted via email.” (**Note:** Administrators can do this via the Microsoft “Trust Center” feature.) Some are precautions you’ve probably been hearing for years, e.g., “If you are using passwords, use strong passwords É and do not reuse passwords for multiple accounts.”

Insurers and other service companies in the cyber space can talk you through appropriate defenses. Beazley, for example, gives prospective clients of their ransomware-related services a questionnaire, developed by them in conjunction with Lodestone Security and KPMG, with questions about email security (e.g. “How often is phishing training conducted to all staff [e.g. monthly, quarterly, annually]?”), internal cybersecurity (e.g., “Do your users have local admin rights on their laptop/desktop?”), and backup and recovery policies (e.g., “Are you able to test the integrity of back-ups prior to restoration to be confident it is free from malware?”).

“Every underwriting question verifies the existence of a protocol or procedure that will stop an event in its tracks,” Dauphinais says. “We want our clients to be thinking about a holistic infrastructure designed to quarantine any such event should it occur.”

Other experts repeat the usual cautions. “All the basics have to be followed,” Friedberg says. That includes “making sure access credentials are changed regularly, multifactor authentication [and] limiting the number of people who have administrative privileges to a system.” Also, use patches as soon as your tech vendors announce them and VPNs for any offsite work. “It’s just that much more significant when people are operating from their own home systems,” Friedberg says.

Experts also say you need to act now. “We’ve been saying for years that you can’t put that off to next year or put it in next year’s budget — you’ve got to do it now,” Hepp urges.

3 tips to protect yourself

- **Segregate backups.** Since hackers are reaching deep into your systems, now’s the time to get serious about doing backups they can’t reach, offline or on the cloud. “Set aside a nightly copy of your backups in such a way that even if your IT team wanted to delete backups, they could not unless they were physically in the room with the backups,” advises Nathan Little, senior vice president of digital forensics and incident response for Tetra Defense in Madison, Wisc. Try to fix it so that as little as possible of your data is available to hackers at any given time.
- **Get aggressive on email.** You might resort to whitelisting protocols that block certain kinds of traffic, though there’s always an efficiency tradeoff there. Temple notes there are “hash hunting” programs that can identify URLs or file “hashes” — an encrypted value that is extracted from the contents of a file or message — in emailed files and block the ones they have reason to believe are malicious. Training staff remains the best line of defense, but you can step that up, too.

“Phishing [vulnerability] is a really easy thing to test with fake emails to see who clicks and who doesn’t,” Dauphinais says.

- **Get help.** Don’t have the IT bandwidth for the job? Call for backup. “Many organizations have popped up in the past year to help providers monitor aberrant activity both at their network firewalls as well as on different computer assets within their network,” Temple says. These companies include vendors of “remote network monitoring, risk modeling, rapid incident response and assistance with disaster recovery and business continuity.”

Resources

- HHS, FBI, and CISA: “Alert (AA20-302A), Ransomware Activity Targeting the Healthcare and Public Health Sector,” Oct. 28: *https://us-cert.cisa.gov/ncas/alerts/aa20-302a*
- CISA Ransomware guide, Sept. 2020: *https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C.pdf*

BACK TO TOP